IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

BLUE SPIKE, LLC *Plaintiff*, v. VERIMATRIX, *Defendant*.	§ § § § § § § §	2:16-cv-00329-RWS LEAD CASE JURY TRIAL DEMANDED
BLUE SPIKE, LLC *Plaintiff*, v. MEDIA SCIENCE INCORPORATED, *Defendant*.	§ § § § § § § § § §	2:16-cv-0701-RWS MEMBER CASE JURY TRIAL DEMANDED

BLUE SPIKE, LLC'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

INTRODUCTION

Not a single construction is in dispute here. Instead, Defendant Media Science Incorporated ("MSI") only argues certain terms are indefinite.[1] However, as shown below the disputed terms are far from indefinite, often utilizing other terms that are core concepts in the field of watermarking technology. MSI appears to be taking the path of least resistance, expending as little effort as possible while hoping the Court will find disputed terms indefinite. This motive is apparent in that certain core watermarking terms with significant support in the specification are implicated; MSI takes issue with basic components of watermarking such as watermarking messages, keys, decoding, and encoding. Additionally, MSI disputes paragraph-sized terms instead of isolating specific portions. Moreover, MSI argues numerous terms are indefinite but opted not to file a motion for summary judgment on indefiniteness. The problem with MSI's approach is that it is burdensome to Blue Spike and not founded in a good faith effort to resolve genuine disputes. Not knowing the basis of MSI's blanket disputes, Blue Spike has been forced to be over-inclusive in its explanations.

This is not the first time MSI has prejudiced Blue Spike with its disregard for this Court's rules. Contrary to the "no excuses" discovery rule, MSI has withheld discovery from the outset of this case. Blue Spike has been forced to forego amending its complaint and reduce its asserted claims without the benefit of a source code review or other relevant discovery. MSI's unilateral

[1] Defendant also raised indefinite arguments pursuant to § 112 (f), but those terms are no

decision to not play by the basic rules of this Court continues to prejudice Blue Spike.

Because no terms are in dispute, the Court need not, and should not, construe any of the disputed terms. Instead, Blue Spike asks the Court to determine all disputed terms are definite and not in need of any construction.

THE PATENTS-IN-SUIT

Each one of the patents-in-suit was invented or co-invented by watermarking innovator Scott Moskowitz. Mr. Moskowitz is the founder and manager of Blue Spike, LLC, as well as the inventor of over 100 patents in the areas of forensic watermarking, signal abstracts, data security, software watermarks, product license keys, deep packet inspection, license codes for authorized software, bandwidth securitization, and others. He is a frequent speaker and prolific author on the subject of digital watermarking. The Patents-in-Suit at issue in this case are examples of Scott Moskowitz' innovations in the area of digital signal processing and watermarking.

APPLICABLE CLAIM CONSTRUCTION STANDARDS

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Lennon Image Techs., LLC v. Macy's Inc.*, 2014 U.S. Dist. LEXIS 105224, at *6 (E.D. Tex. Aug. 1, 2014); *Light Transformation Techs. LLC v. Lighting Sci. Group Corp.*, 2014 U.S. Dist. LEXIS 94090, at *10 (E.D. Tex. July 10, 2014) (*quoting Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc)). The specification "'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Light Transformation Techs. LLC*, 2014 U.S. Dist. LEXIS 94090, at *11. The prosecution history also supplies intrinsic evidence if it is in evidence. *Lennon Image Tech., LLC*, 2014 U.S. Dist. LEXIS 105224 at *7. "Differences among the claim terms can also assist in understanding a term's meaning . . . . For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation." *Alcatel United States Res., Inc. v. Microsoft Corp.*, 2008 U.S. Dist. LEXIS 49615, at *5 (E.D. Tex. Jun. 27, 2008). "Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent." *Id.* at *7. Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

LEVEL OF ORDINARY SKILL IN THE ART

Blue Spike, LLC ("Blue Spike") proposes that a person of ordinary skill in the art would have a Master's degree in computer science or computer engineering, or equivalent experience, as well as two years experience in the field of digital watermarking and cryptography. Digital watermarking and cryptography experience are highly relevant considering some terms in the patents-in-suit are readily understandable to one having experience in digital watermarking and cryptography.

ARGUMENT

I. "the water mark message"

Blue Spike's Construction	**Defendant's Construction**
Proposed Construction: Plain and Ordinary Meaning	Indefinite

The term "water mark message" needs no construction. It is a term that is readily understood in the art as "the watermark information encoded within a digital signal." Declaration of Yannis Papakonstantinou ("Papakonstantinou Decl.") at 11, ¶ 11(a). Dr. Papakonstantinou, a Stanford graduate and professor of Computer Science and Engineering at the University of California, San Diego, explains that "a digital signal is watermarked with a watermark message." *See Realtime Data, LLC d/b/a IXO v. Packeteer, Inc., et al.*, Case No. 6:08-cv-144-LED-JDL Dkt. No. 371, at * 28 (E.D. Tex. June 22, 2009) ("[T]he lay meaning of this term is the same meaning as that which a person having ordinary skill in the art would attribute to the term."), *attached as* Exhibit 1. "The term 'watermark' and 'watermark message' are often used interchangeably." Papakonstantinou Decl. at 11, ¶ 11(a).

One of ordinary skill in the art understands this common watermarking term, thus it should not be construed.

The specification supports Blue Spike's position. "The specification describes how a 'watermark location is determined . . . on the creation of a pseudo-random key.'" Papakonstantinou Decl. at 3, ¶ 11(b) (citing '868 Patent, Col. 7, ll. 29-31). "Three concepts are described here: the watermark message (here referred to as a 'watermark'), the key, and the location to place the watermark." *Id.* at 3-4. "Shortly thereafter, the specification explains how 'an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of the watermark message and the most suitable area and method of insertion.'" *Id.* at 4 (citing '868 Patent, Col. 7, ll. 35-39). "Here we see the same three concepts as in the earlier portion of the specification, only 'watermark message' is used instead of 'watermark.'" *Id.*; *see also*, '868 Patent, Col. 7, ll. 57-60 (describing the relationship between the watermark, or watermark message, and key: "The number of bits in the primary key should match or exceed the number of bits in the watermark message."). "These references clearly describe the watermark message's use, thus the term needs no construction." Papakonstantinou Decl. at 4, ¶ 11(b).

Blue Spike also provided extrinsic evidence in support of its position. For example, the term "watermark" has also been defined as "[a] general term that can refer to *an embedded message*, a reference pattern, a message pattern, or an added pattern." Al_Dawla, STEGANOGRAPHY ENHANCEMENT BY COMBINING TEXT AND IMAGE THROUGH IMAGE PROCESSING TECHNIQUES, Dissertation, *attached as* Exhibit 2. As shown here, the embedded message is the watermark message.

This term is not indefinite and needs no construction. See Papakonstantinou Decl. at 5, ¶ 11(e). Because Defendant argues no alternative construction, this term should not be construed. *See* Ex. 1, *Realtime Data v. Packeteer*, Case No. 6:08-cv-144-LED-JDL, Dkt. No. 371, at * 55 n.37 ("Defendants did not offer a proposed construction for this term, relying solely on their Indefiniteness Motion. (Cite). Having resolved the dispute regarding whether this claim term is indefinite, the Court declines to adopt a construction at this point.").

II. "wherein the plurality of codecs is selected based on a predefined criterion comprising one of the group consisting of: robustness, imperceptibility, security, said codec's association with the encoding of at least one watermark, upgradability, variance of encode or decode functions, and combinations thereof"

Blue Spike's Construction	**Defendant's Construction**
<u>*Proposed Construction*</u>: Plain and Ordinary Meaning	Indefinite

As a threshold issue, Defendant's dispute over this term is improper. *See also* Section IV. Defendant disputes this term generally without identifying the specific portion it considers indefinite. This is improper and prejudicial to Blue Spike for a number of reasons. First, it unnecessarily increases Blue Spike's briefing costs. Second, it allows Defendant to employ a see-if-it-sticks approach rather than a good-faith argument narrowed to a specific term. Finally, it allows Defendant to choose a single argument after Blue Spike has been forced to defend itself on multiple fronts. Blue Spike asks the Court to decline to construe this over-inclusive term.

In response to Defendant's over-inclusiveness approach, Blue Spike will dissect the term as best it can into its component parts. That being said, Blue Spike reserves the right to cite to tailored evidence in the event Defendant narrows its argument in its response. At bottom, this term is definite and comprised of terms readily understood by one of ordinary skill in the art.

- ***Codec.*** The term "codec" is not a novel term. "One of ordinary skill in the art understands that a codec allows for the encoding and decoding of a signal." Papakonstantinou Decl. at 5, ¶ 12(b). This is also how the patent specification defines the term. '609 Patent, Col. 20, ll. 49-50 ("a new CODEC (encoder/decoder)"). And the Electrical Engineering Dictionary lends support for this definition, defining "codec" as a "word formed from encoder and decoder. A device that performs encoding and decoding communications protocols." Electrical Engineering Dictionary, 2000, *attached as* Exhibit 3. This term is not indefinite and needs no construction.
- ***Robustness.*** "Robustness" is a term common to digital watermarking. "One of ordinary skill in the art understands that

a watermark may be considered robust if it is able to withstand certain common operations that may alter the watermarked signal." Papakonstantinou Decl., at 5-6 ¶ 12(c). This term also finds support in the specification where "'differences in robustness' may be determined because 'a sample window size of 15 seconds can be compared to an implementation using a sample window size of 45 seconds.'" Papakonstantinou Decl. at 5-6, ¶ 12(c) (quoting '609 Patent, Col. 19, ll. 59-64). "Robustness" has also been defined as the "ability of steganography to survive signal-processing operations." Ex. 2 at 186. And the definition of "transformation analysis" shows that there are degrees of robustness. Ex. 2 at 189 ("The goal is to produce a more robust watermark."). Additionally, the definition of "invisible watermark" shows that there are two broad categories of watermarks, indicating a spectrum of fragile to robust or weak to strong: "fragile and robust." Ex. 2 at 182. This term is not indefinite and needs no construction.

- ***Imperceptibility.*** This term is definite, and it has a specific meaning in the context of watermarking. "One of ordinary skill in the art understands that it is often the goal of watermarking to make a watermark message imperceptible." Papakonstantinou Decl. at 5, ¶ 12(d). The specification supports this definition, describing how "the design goal of the present invention in preanalyzing a signal to mask the digital watermarks make imperceptibility possible." '609 Patent, Col. 15, ll. 64-66. Extrinsic evidence supports this position. "Imperceptible" has been defined as "undetectable by a human perceptual system." Ex. 2 at 181. And "transparent watermark" has been defined as an "imperceptible watermark." Ex. 2 at 189. Finally, "watermarking" has been defined as the "practice of imperceptibly altering a Work to embed a message[2] about that work." Ex. 2 at 190. This term is not indefinite and needs no construction.

- ***Security.*** This term has a common definition in the field of watermarking. "One of ordinary skill in the art understands that another common watermarking goal, especially in certain contexts such as copyright protection, is that of security, a term that describes how an attacker may know how an embedding algorithm operates but will still not be able to locate the watermark message without the watermark key." Papakonstantinou Decl. at 6, ¶ 12(e). A method for improving watermarking security is described in the patent's specification: "The second method for varying of the encoding/decoding algorithms corresponds to increased security . . . . In this method, the Framework selects a new CODEC, from among a list of

[2] *Note* – here the term "message" is the watermark message.

predefined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark." '609 Patent, Col. 20, l. 65 – Col. 21, l. 6. Extrinsic evidence supports Blue Spike's position. "Security" has been defined as the "ability of a steganography to resist intentional tampering." Ex. 2 at 187. This term is not indefinite and needs no construction.

- ***Said codec's association with the encoding of at least one watermark; variance of encode or decode functions.*** The association of codecs and watermarks and variance of encode/decode functions is discussed throughout the patent. For example, the patent teaches methods "for varying of the encoding/decoding algorithms," and how "a new CODEC" may be selected "from among a list of pre-defined CODECs", associating with each change a new CODEC with the watermark. '609 Patent, Col 20, ll. 40-52. Another method teaches how "the Framework selects a new CODEC, from among a list of predefined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark." '609 Patent, Col. 21, ll. 2-6. The specification describes how "varying of the encoding/decoding algorithms corresponds to increased security." '609 Patent, Col. 20, ll. 65-66.

These terms are definite, sufficiently described in the patent, and need no construction.

- ***Upgradability.*** "One of ordinary skill in the art understands that something that is upgradable is capable of being improved." Moreover, the '213 Patent provides further support for upgrading a watermarking system: "This ability can be used to provide upgrades to the watermark system, without breaking support for decoding watermarks created by previous versions of the system." '213 Patent, Col. 3, ll. 55-58. This term is not indefinite and needs no construction.
- ***Variance of encode or decode functions.*** This term has been explained above. This term is not indefinite and needs no construction.
- ***Wherein the plurality of codecs is selected based on a predefined criterion.*** In light of the above, this phrase needs no explanation. The phrase describes how a codec is selected to operate on a watermark based on one of the above criteria, e.g. robustness or security. This term is not indefinite and needs no construction.

As described here, this term and its component parts are definite. *See* Papakonstantinou Decl. at 8, ¶ 12(i). Because Defendant argues no alternative construction, this term should not be construed. *See* Ex. 1, *Realtime Data v.*

Packeteer, Case No. 6:08-cv-144-LED-JDL, Dkt. No. 371, at * 55 n.37 (declining to construe a term after resolving indefiniteness dispute because defendant had not proposed an alternate definition).

III. "detecting and/or decoding at least one watermark from an encoded content signal"

Blue Spike's Construction	**Defendant's Construction**
Proposed Construction: Plain and Ordinary Meaning	Indefinite

Once again, it is unclear what aspect of this term Defendant specifically believes is indefinite. As noted above under the term "water mark message," one of ordinary skill in the art understands that "watermark information [is] encoded within a digital signal." Papakonstantinou Decl. at 3, ¶ 11(a). Further, "one of ordinary skill in the art understands that a watermark message is encoded into a digital signal and later decoded from the same signal. The patent describes how different encoding and decoding algorithms may be used. For instance, the specification describes 'the architecture to provide automated variance of algorithms to encode and decode a single watermark.'" Papakonstantinou Decl. at 7-8, ¶ 12(h). It may also be desirable to detect an embedded watermark before decoding, or instead of decoding altogether. The specification teaches how this is "made possible for parties possessing a decoded to verify the presence of watermarks in a data stream, without accessing the contents of the watermark." '213 Patent, Col. 3, ll. 35-38. The patent also teaches how it "would be possible to scan or search archives for files containing watermarked content, and to verify the validity of the presence of such files in an archive, by means of the information contained in the watermarks." '213 Patent, Col. 3, ll. 38-41. Blue Spike's position is supported by the extrinsic record. For instance, a "watermark decoder" has been defined as the "portion of a watermark detector that maps extracted marks into messages. In most cases this is the entire operation of the watermark detector." Ex. 2 at 190. And a "watermark detector" has been defined as a "hardware device or software application that detects and decodes a watermark." Ex. 2 at 190.

As described here, this is not indefinite. *See* Papakonstantinou Decl. at 9, ¶ 13(d). Because Defendant argues no alternative construction, this term should not be construed. *See* Ex. 1, *Realtime Data v. Packeteer*, Case No. 6:08-cv-144-LED-JDL, Dkt. No. 371, at * 55 n.37 (declining to construe a term after resolving indefiniteness dispute because defendant had not proposed an alternate definition).

IV. "wherein . . . selected from a group comprising: a random key; a candidate key; a pseudo-random key; a watermark key; a watermarking key; a private key; a public key; a semiprivate key; a master framework key; a private key; and a digital watermark key."

Blue Spike's Construction	Defendant's Construction
Proposed Construction: Plain and Ordinary Meaning	Indefinite

As a threshold issue, Defendant's dispute over this term is improper. *See also* Section II. Defendant disputes this term generally without identifying the specific portion it considers indefinite. This is improper and prejudicial to Blue Spike for a number of reasons. First, it unnecessarily increases Blue Spike's briefing costs. Second, it allows Defendant to employ a see-if-it-sticks approach rather than a good-faith argument narrowed to a specific term. Finally, it allows Defendant to choose a single argument after Blue Spike has been forced to defend itself on multiple fronts. Blue Spike asks the Court to decline to construe this over-inclusive term.

In response to Defendant's over-inclusiveness approach, Blue Spike will dissect the term as best it can into its component parts. That being said, Blue Spike reserves the right to cite to tailored evidence in the event Defendant narrows its argument in its response. At bottom, this term is definite and comprised of terms readily understood by one of ordinary skill in the art. Nevertheless, this term is definite and comprised of terms readily understood by one of ordinary skill in the art.

- ***A watermark key; a watermarking key; a digital watermark key.*** Watermark keys are fundamental to watermarking technology and readily understood by one of ordinary skill in the art. One of ordinary skill in the art understands that "a watermark message may be embedded and later found by a key." Papakonstantinou Decl. at 4, ¶ 11(d). This term is not indefinite and needs no construction.
- ***Random key; pseudo-random key.*** "It is understood by one of ordinary skill in the art that 'random' implies that the key is created arbitrarily, i.e. not by pattern, while a pseudo random key only appears to have been created arbitrarily." Papakonstantinou Decl. at 10, 14(c). The specification teaches how "[d]igital watermarks can be encoded with random or pseudo-random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark." '213 Patent, Col. 3, ll. 14-17. This term is not indefinite and needs no construction.
- ***A candidate key.*** The term "candidate key" is "readily understood by one of ordinary skill in the art" and "implies a

given key is a candidate that may be used in an attempt to encode or decode a watermark." Papakonstantinou Decl. at 11, ¶ 14(e). The term "candidate key" is described in Applied Cryptography as one of many keys that may potentially decode a watermark. *See* Schneier, APPLIED CRYPTOGRAPHY, Jan. 1996, at 156, 266, and 303, *attached as* Ex. 5. The extensive Applied Cryptography reference is incorporated into the specification as a reference to the '213 patent. *See* Ex. 6, '213 patent, page 3; *see also* U.S. Patent 8,774,216, U.S. Patent 7,830,915, U.S. Patent 7,362,775, U.S. Patent 7,770,017 and U.S. Patent 7,779,261.

- ***Master Framework Key.*** The term "master framework key" is found in various patents also attributed to the inventor of the patents-in-suit. "According to an advantageous embodiment of the present invention, an active scheme is implemented which is described as follows. The farthest party upstream, who presumably controls the ultimate copyrights and distribution rights of the data generates two keys. The first key is a regular watermark key, as described in previous related patent application disclosures by The DICE Company, particularly, including the 'Method for Stega-Cipher Protection of Computer Code' application. This key is used for actual encoding and decoding of information from the watermark channel 'owned' by this party. The second key is a new type of watermark key, called a master framework key, which dictates how the entire data stream in general is to be packetized; how the data stream packets are to be allocated among a predetermined number of reserved watermark channels; and how the channels are to be assigned to downstream parties." *See* Ex. 7, U.S. Patent 8,774,216, Col. 20, l. 53 – Col. 21, l. 10; Ex. 8, U.S. Patent 7,830,915, Col. 20, l. 57 – Col. 21, l. 17; and U.S. Patent 7,362,775, Ex. 9, Col. 21, ll. 5-45.

- ***A private key; a public key; a semiprivate key.*** Private, public, and semiprivate keys are well known terms in the art of cryptography and watermarking. A "private key" is defined as a "cryptographic key used with a public key cryptographic algorithm which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key." Ex. 2 at 146. In a system that includes not just public and private but also semiprivate keys, the public key allows one to verify that a watermark exists but not decode it; a semiprivate key allows one to authenticate and decode the watermark but not create a new one; and a private key allows one to create a new watermark.[3]

[3] For more information on public, private, and semiprivate keys, *see* https://moderncrypto.org/mail-archive/curves/2014/000068.html; *see also* *https://tahoe-*

The specification describes how these keys are used: "The present invention relates to methods for the management and distribution of digital watermark keys (e.g. private, semiprivate and public) and the extension of information associated with such keys in order to create a mechanism for the securitization of multimedia titles to which the keys apply." '213 Patent, Col. 5, ll. 32-36. More than this, the patent provides the following in-depth discussion of private, semiprivate, and public keys:

> Multichannel watermarks with **private, semiprivate and public keys** used as different levels of neighboring rights assist in the creation of a self-contained model for the exchange of copyrighted works. **Private key watermarks** can be inserted into content to establish ownership rights (copyright, master right, etc.) with the content creator or an agent of the content creator maintaining control over the key. **Semiprivate watermark keys** can exist in a separate channel of the information signals that make up the work to be exchanged for subsequently delegating responsibility to distributors or sales entities to restrict resale rights in the same manner that physical goods have an exchange of title corresponding to their sale. And finally, **public watermark keys** exist as an independent component of the identification, authentication or advertising of a given work to be widely distributed over networks for initiating the purchase of a sought-after work.

lafs.org/pipermail/tahoe-dev/2009-July/002371.html (drafted by cryptography legend Harold "Hal" Finney who was a developer of the Pretty Good Privacy (PGP) encryption software and the first recipient of a bitcoin from the bitcoin developer Satoshi Nakamoto).

> ’213 Patent, Col. 5, ll. 1-16. “And the patent also distinguishes these terms from their more common use in the context of encryption: ‘To differentiate the present invention from the art of public key cryptography, use of private, semiprivate, and public keys refers only to the use of such information with the stated purpose of distributing goods and watermarking content, not encryption or cryptography in the general sense.” Papakonstantinou Decl. at 10, ¶ 14(d) (citing ’213 Patent, Col. 5, ll. 37-41). These terms are not indefinite and need no construction.

As described here, this is not indefinite. *See* Papakonstantinou Decl. at 13, ¶ 15(b). Because Defendant argues no alternative construction, this term should not be construed. *See* Ex. 1, *Realtime Data v. Packeteer*, Case No. 6:08-cv-144-LED-JDL, Dkt. No. 371, at * 55 n.37 (declining to construe a term after resolving indefiniteness dispute because defendant had not proposed an alternate definition).

V. “the key used for decoding”

Blue Spike’s Construction	**Defendant’s Construction**
Proposed Construction: Plain and Ordinary Meaning	Indefinite

As noted above under the term “water mark message,” one of ordinary skill in the art understands that “a key may be used to decode a watermark.”

Papakonstantinou Decl. at 12, ¶ 15(a). A "watermark information [is] encoded within a digital signal." Papakonstantinou Decl. at 3, ¶ 11(a). Further, "one of ordinary skill in the art understands that a watermark message is encoded into a digital signal and later decoded from the same signal. The patent describes how different encoding and decoding algorithms may be used. For instance, the specification describes 'the architecture to provide automated variance of algorithms to encode and decode a single watermark.'" Papakonstantinou Decl. at 7-8, ¶ 12(h).

The specification explains: ""Digital watermarks can be encoded with random or pseudo-random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark." '213 Patent, Col. 3, ll. 14-17. Dr. Papakonstantinou explains that this description in the specification "shows how a key is necessary to decode a watermark that has been encoded with random or pseudo-random keys." Papakonstantinou Decl. at 12, ¶ 15(a).

As described here, this is not indefinite. *See* Papakonstantinou Decl. at 13, ¶ 15(b). Because Defendant argues no alternative construction, this term should not be construed. *See* Ex. 1, *Realtime Data v. Packeteer*, Case No. 6:08-cv-144-LED-JDL, Dkt. No. 371, at * 55 n.37 (declining to construe a term after resolving indefiniteness dispute because defendant had not proposed an alternate definition).

VI. "wherein the step of detecting and/or decoding . . . is separate from the encoding process"

Blue Spike's Construction	Defendant's Construction
<u>*Proposed Construction*</u>: Plain and Ordinary Meaning	Indefinite

The detecting, decoding, and encoding processes of digital watermarking have already been addressed above. In regards to the detecting and/or decoding steps being separate from the encoding step, there is significant support for this separation in the specification. For example, the specification explains how it "is also desirable to separate the functionality of the decoder side of the process to provide fuller recognition and substantiation of the protection of goods that are essentially digitized bits, while ensuring the security of the encoder and the encoded content." '213 Patent, Col 3, ll. 27-32. The specification also describes how "[s]eparating the decoder from the encoder can limit the ability to reverse the encoding process while providing a reliable method for third parties to be able to make attempts to screen their archives for watermarked content without being able to tamper with all of the actual watermarks." '213 Patent, Col. 11, ll. 32-26. And the patent's specification further explains how this might be accomplished

> by placing separate signals in the content using the encoder, which signal the presence of a

> valid watermark, e.g. by providing a "public key accessible" watermark channel which contains information comprised of a digitally signed digital notary registration of the watermark in the private channel, along with a checksum verifying the content stream. The checksum reflects the unique nature of the actual samples which contain the watermark in question, and therefore would provide a means to detect an attempt to graft a watermark lifted from one recording and placed into another recording in an attempt to deceive decoding software of the nature of the recording in question. During encoding, the encoder can leave room within the watermark for the checksum, and analyze the portion of the content stream which will contain the watermark in order to generate the checksum before the watermark is encoded. Once the checksum is computed, the complete watermark certificate, which now contains the checksum, is signed an/or encrypted, which prevents modification of any portion of the certificate, including the checksum, and finally encoded into the stream. Thus, if it is somehow moved at a later time, that fact can be detected by decoders.

Col. 11, ll. 36-68.

As described here, this is not indefinite. *See* Papakonstantinou Decl. at 14, ¶ 17. Because Defendant argues no alternative construction, this term should not be construed. *See* Ex. 1, *Realtime Data v. Packeteer*, Case No. 6:08-cv-144-LED-JDL, Dkt. No. 371, at * 55 n.37 (declining to construe a term after resolving indefiniteness dispute because defendant had not proposed an alternate definition).

CONCLUSION

It is evident that the disputed terms are well understood in the art and/or sufficiently described in the patent specifications. Defendant's shotgun approach of declaring various terms indefinite is both unsubstantiated and unhelpful to the claim construction process. Defendant has proposed no alternative constructions, thus no term should be construed.

Respectfully submitted,

/s/ Randall T. Garteiser
Randall T. Garteiser
Lead Attorney
Texas Bar No. 24038912
rgarteiser@ghiplaw.com
Christopher A. Honea
Texas Bar No. 24059967
chonea@ghiplaw.com
GARTEISER HONEA, P.C.
119 W Ferguson St
Tyler, Texas 75702
(888) 908-4400 phone/fax

Kirk J. Anderson
California Bar No. 289043
kanderson@ghiplaw.com
Ian N. Ramage
California Bar No. 224881
iramage@ghiplaw.com
GARTEISER HONEA, P.C.
44 North San Pedro Road
San Rafael, California 94903
(888) 908-4400 phone/fax

Counsel for Blue Spike, LLC

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, this document was served on all counsel who are deemed to have consented to electronic service. Local Rule CV-5(a)(3)(A). Pursuant to Federal Rule of Civil Procedure 5(d) and Local Rule CV-5(d) and (e), all other counsel of record not deemed to have consented to electronic service were served with a true and correct copy of the foregoing by email.

/s/ Randall Garteiser